



CVE-2019-11249

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-11249
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-29 01:15:00 UTC
Updated	2020-10-02 16:45:00 UTC
Description	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Ku

Risk And Classification

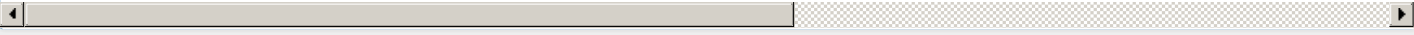
Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Redhat	Openshift Container Platform	3.10	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.9	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	3.10	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.9	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All

References

Reference
CVE-2019-11249: Incomplete fixes for CVE-2019-1002101 and CVE-2019-11246, kubectl cp potential directory traversal · Issue #80984 · kub

Red Hat Customer Portal
September 2019 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal
Google Groups
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit
Discovery Credit
LEGACY: Yang Yang, Amazon
Legacy QID Mappings
377864 Kubernetes Kubectl Potential Directory Traversal Vulnerability
501590 Alpine Linux Security Update for k3s